DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY GARRISON, ALASKA AND FORT RICHARDSON (PROV)
Fort Richardson, Alaska 99505-6000

United States Army Garrison, Alaska Regulation 380-6 **14 September 2006**

Security

Industrial Security Program

Summary. This regulation contains guidance covering the Industrial Security Program which is managed by the US Army Garrison, Alaska and Fort Richardson (USAG-AK), Installation Security & Intelligence Office (ISIO).

Applicability. This regulation applies to USAG-AK and United States Army Alaska (USARAK) units and activities and all other activities, organizations, and agencies located at or in the geographical areas of Forts Richardson and Wainwright.

Interim changes. Interim changes to this regulation are not official unless the Director of Information Management (DOIM) authenticates them. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested improvements. This regulation's proponent agency is the USAG-AK, ISIO. Users are invited to send comments and suggested improvements on a Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) directly to IMPA-FRA-PLS, Fort Richardson, AK.

Contents

1. Purpose.
The purpose of this regulation is to provide instructions and policy guidance on the following:

a. USAG-AK Industrial Security Program (hereby referred to as program).

b. Department of Defense Form 254 (DD 254).

c. Contractor Verification System (CVS).

2. References
Required and related publications, prescribed and referenced forms, and related web sites are listed in appendix A.

3. Explanation of abbreviations.
The abbreviations used in this regulation are listed in the glossary.

4. Responsibilities.

a. The Chief, ISIO, as the commander's representative for all Industrial Security matters, will:

(1) Administer the program.

(2) Serve as the Installation Point of Contact for CVS.

(3) Appoint Trusted Agent Security Managers (TASMs).

b. The Security Specialist (Industrial), ISIO will:

(1) Serve as the subject matter expert for the program.

(2) Serve as the TASM for CVS.

(3) Maintain Joint Personnel Adjudication System (JPAS) account for submission of visit requests for Industry personnel.

(4) Appoint Trusted Agents (TAs) for CVS.

c. The Contracting Officer Representative (COR) or Government Program Manager (PM) will:

(1) Include provisions directing the contractor and contractor employees to comply with the requirements of this regulation in all Statements of Work (SOW) or purchase requests for contracts involving classified information or access to Government information systems.

(2) Oversee contractors working in support of the organization.

(3) Serve as the TA for CVS.

(4) Ensure contractor personnel meet minimum investigative requirements for DoD computer access prior to entering into CVS.

(5) Liaise with the Facility Security Officer (FSO), the Contractor Personnel Representative, the Regional Contracting Office (RCO) and the Security Specialist (Industrial).

d. Facility Security Officer (FSO) will serve as the contractor's representative for all classified contracts on the installation. FSOs will:

(1) Provide a copy of the contract, including the DD 254, to the Security Specialist (Industrial).

(2) Ensure security information for all contractor personnel is current in JPAS (to include granting access).

(3) Submit visit requests for contactor personnel to the Security Specialist (Industrial) via JPAS. Submit updated visit requests as needed (i.e. when personnel access status changes, personnel removed from the contract, new personnel added).

(4) Provide, or have the individual provide, information to the TA required by CVS for the issuance of Common Access Cards (CACs).

(5) Ensure all contractor personnel turn-in CACs to the TA prior to termination from or expiration of the contract.

e. Contractor Personnel Representative (CPR) will serve as the contractor's representative for all unclassified contracts on the installation. The CPR should be someone within the contractor's organization who is familiar with the contract and personnel. Duties include:

(1) Provide, or have the individual provide, information to the TA required by CVS for the issuance of Common Access Cards (CACs).

(2) Ensure all contractor personnel turn-in CACs to the TA prior to termination from or expiration of the contract.

f. USAG-AK, Director of Human Resources (DHR) will:

(1) Issue CACs to contractor personnel who have been entered into Defense Enrollment Eligibility Reporting System (DEERS).

(2) Serve as the Point of Contact for turn-in of all contractor CACs.

g. For all contracts solicited through the Regional Contracting Office, Alaska (RCO-AK) that require access to classified information or access to government computer systems, RCO-AK will:

(1) Submit all DD 254s to the Security Specialist (Industrial) for approval prior to a contract being solicited. Submit all DD 254s to the Security Specialist (Industrial) for approval before the contract is amended.

(2) Provide contractors with link to or copy of this regulation when contract is awarded/amended.

(3) For all classified contracts, provide the Security Specialist (Industrial) and COR/PM with name of FSO (when contract is awarded/amended).

(4) For all unclassified contracts, provide the Security Specialist (Industrial) and COR/PM with name of CPR (when contract is awarded/amended).

h. The 59th Signal Battalion/Director of Information Management (59th SIG BN/DOIM):

(1) Oversees the Information Assurance program in Alaska.

(2) Provides guidance on investigation requirements for access to government-owned computer systems.

5. Security oversight of classified contracts performed on USAG-AK installations.
Security of contracts performed on the installation is normally provided by the ISIO. Exceptions are when:

a. The contract is performed on behalf of non-supported tenants. In these cases, user agency's security manager will perform security oversight of the contract.

b. The Garrison Commander has elected not to assume cognizance over the contract. In these cases, security cognizance will be performed by the Defense Security Service.

c. The contract involves Sensitive Compartmented Information (SCI). In these cases, oversight will be provided by the USARAK Special Security Officer (SSO).

6. Security requirements.
All classified contracts in support of USAG-AK or supported tenant organizations/units shall include provisions requiring contractors performing on classified contracts to abide by DoD, DA, and local security policies and procedures. Solicitations shall include a copy of this regulation or a link to this regulation. Unit Security Managers and Facility Security Officers will work together to ensure that contractors understand their responsibilities to properly handle classified information and receive security training as required by DA and local policy.

7. Inspections.
Compliance inspections for classified contractors will be provided by the ISIO as part of the annual security inspection (ASI) program. An industrial security checklist will be added to the Garrison Security portion of the USARAK Organizational Inspection Program (OIP) and USAG-AK ASI checklists. Oversight of CVS will be included as part of the Industrial Security program checklist.

8. Compromises.
All losses, compromises, or suspected compromises of classified information will be immediately reported to the Security Specialist (Industrial). In accordance with (IAW) the USARAK/USAG-AK Security SOP, an Initial Incident Report will be submitted to the ISIO no later than the close of the next business day.

9. Classified contract specifications—DD 254.
Contracts which require personnel to access classified information must include a DD 254. The RCO will ensure that all DD 254s are routed through the Security Specialist (Industrial) for approval prior to the contract being solicited. All updates or amendments to the DD 254 must also be approved prior to finalization. The DD 254 will be filled out in its entirety and will include the following information (as applicable). A sample can be found on the ISIO's website.

a. Block 6 (Contractor). Contractor's corporate address (part a) and DSS Industrial Security Field Office (part c) will be used to complete these blocks.

b. Block 8 (Actual Performance). Address of installation organization which the contract is supporting (part a) and ISIO's address (part c) will be used to complete these blocks.

c. Block 9 (General Identification of This Procurement). A brief, unclassified description of the contract will be included in this block.

d. Blocks 10 and 11. All blocks require a "yes" or "no" answer.

e. Block 13. Specific security guidance will be included in this block. If not all contractor personnel require access to classified information, only those positions that do require access will be identified (by position title) in this block.

f. Block 17. The Contracting Officer (KO) or other authorized personnel from the RCO will sign the DD 254. RCO personnel are the only personnel authorized to sign the DD 254.

10. Contract award notifications.
RCO-AK will notify the Security Specialist (Industrial) upon the awarding of classified contracts and unclassified contracts requiring computer access. This notification will include contact information for the FSO (in the case of a classified contract) or the CPR (in the case of contracts only requiring computer access).

11. Requirements for access to government-owned computer systems
All contracts in which contractors access government-owned computer systems must include a provision requiring the contractor to abide by all policies and training requirements as issued by the 59th SIG BN/DOIM.

12. Investigation/Access verification.
Verification procedures for contractors requiring access to classified information or a favorable background investigation shall be included in all applicable contracts. The verification procedures

a. Contractors with an investigative requirement. Contractors who require a favorable background investigation in order to perform the duties of the contract (i.e. those working guard duties or those who require access to government-owned computer systems) must have the investigation verified through JPAS. This verification, which should be conducted by the unit security manager, must occur prior to the TA entering the contractor into CVS. Detailed instructions for CVS are found in paragraph 13.

b. Contractors requiring access to classified information. Contractors who require access to classified information must have their access verified prior to contract performance. Access verification will occur via a visit request in the Joint Personnel Adjudication System (JPAS). This visit request will be sent to both the Security Specialist (Industrial) and the unit Security Manager's JPAS account. JPAS account for the Security Specialist (Industrial) is W4UJAA-CON.

c. Updates. FSOs are required to notify the Security Specialist (Industrial) of any changes in status for their personnel. Notification will be made via email message or phone call within three (3) days of the change of status. Notification will be followed by updated visit request message sent to both parties listed in paragraph (b). Change of status information which must be reported includes:

(1) Loss of access to classified information or other change in cleared employee status IAW DoD 5220.22-R, paragraph 1-302c.

(2) Discovery of reportable information IAW DoD 5220.22-R, paragraph 1-302a.

13. CVS.
Management of the CVS is an integral part of the Industrial Security Program. All personnel assigned roles in the CVS program must ensure that the procedures listed below are followed.

a. Uncleared contractors (i.e., contractors not requiring access to classified information) requiring a CAC. CVS will be used for the issuance of CACs for uncleared contractor personnel. The CVS procedures for issuance are as follows:

(1) The COR/PM will submit a request to be appointed as a TA in CVS. This request will be submitted to the TASM and will include the COR/PMs full name and social security number (required for the issuance of an account).

(2) The TA will schedule a desk-side training session with the TASM. At the session, the TA's logon and password will be issued.

(3) Before entering the individual into CVS, the TA will verify with the unit Security Manager that the minimum investigative requirements have been met. The Security Manager will printout the individual's JPAS screen for the TA to maintain as proof. This printout will be maintained for the duration of the contract.

(4) After the contractor completes his portion of the CVS application, the TA will verify the information and, if correct, approve the application.

(5) The contractor's information must be re-verified every six months. It is the TA's responsibility to re-verify their contractors when notified. Failure to re-verify the contractor will result in the withdrawal of the individual's CAC certificates.

(6) When a contractor's employee leaves the organization (e.g., separation from the contractor's employ, or the end of the contract), the TA will collect the CAC. The TA will then return all CACs to the ID Card section of the DHR for destruction.

b. Cleared contractors (i.e., contractors requiring access to classified information) requiring a CAC. Although similar, the procedures for contractors working on classified contracts do differ. The CVS procedures for the issuance of CACs to cleared contractors are as follows:

(1) The COR/PM will submit a request to be appointed as a TA in CVS. This request will be submitted to the TASM and will include the COR/PMs full name and social security number (required for the issuance of an account).

(2) The TA will schedule a desk-side training session with the TASM. At the session, the TA's logon and password will be issued.

(3) Before entering the individual into CVS, the TA will verify with the unit Security Manager that the minimum investigative requirements have been met. Since the investigative requirement for classified access is equal or greater than the network access requirements, the TA will maintain a copy of the Security Manager's visit request printout as proof. This printout will be maintained for the duration of the contract.

(4) After the contractor completes his portion of the CVS application, the TA will verify the information and, if correct, approve the application.

(5) The contractor's information must be re-verified every six months. It is the TA's responsibility to re-verify their contractors when notified. Failure to re-verify the contractor will result in the withdrawal of the individual's CAC certificates.

(6) When a contractor's employee leaves the organization (e.g., separation from the contractor's employ, or the end of the contract), the TA will collect the CAC. The TA will then return all CACs to the ID Card section of the DHR for destruction.

c. System Integrity. It is the TASMs responsibility to help ensure the integrity of CVS by removing all unnecessary users. Units/organizations hosting contractors will assist by:

(1) Notifying the TASM of any change in COR. Notification will be made within 72 hours and will include the new CORs information (full name and SSN).

(2) Notifying the TASM of any contract cancellations, expirations, or other discontinuance. The notification will be made within 72 hours and will include, if applicable, information regarding the new contractor and COR.

OFFICIAL:

DAVID L. SHUTT
COL, AR
Commanding

JEFFERY R. SCHILLING
LTC, SC
Director of Information Management

DISTRIBUTION:
A copy of this regulation can be found at http://www.usarak.army.mil/publications/.

Appendix A
References

Section I
Required Publications

AR 380-5 ..... Department of the Army Information Security Program

AR 380-49 ..... Industrial Security Program

AR 380-67 ..... Personnel Security Program

..... USARAK/USAG-AK Security SOP

Section II
Related Publications

DOD 5220.22R ..... Industrial Security Regulation

Section III
Prescribed Forms

None

Section IV
Referenced Forms

DA Form 2028 (Recommended Changes to Publications and Blank Forms) is cited in the suggested improvements paragraph.

DD Form 254

Section V
Related Web Sites

USAG-AK ISIO website https://richardson.ak.pac.army.mil/isio

CVS website https://www.dmdc.osd.mil/apppj/cvs/index.jsp

Glossary

ASI ..... Annual Security Inspection

AR ..... Army Regulation

CAC ..... Common Access Card

COR ..... Contracting Office Representative

CPR ..... Contractor's Personnel Representative

CVS ..... Contractor Verification System

DA ..... Department of the Army

DD ..... Defense Department

DEERS ..... Defense Enrollment Eligibility Reporting System

DHR ..... Director of Human Resources

DoD ..... Department of Defense

DOIM ..... Director of Information Management

FSO ..... Facility Security Officer

IAW ..... In Accordance With

ID ..... Identification

ISIO ..... Installation Security and Intelligence Office

JPAS ..... Joint Personnel Adjudication System

KO ..... Contracting Officer

OIP ..... Organizational Inspection Program

PM ..... Program Manager

RCO ..... Regional Contracting Office

SOP ..... Standing Operating Procedure

SSO ..... Special Security Office

TA ..... Trusted Agent

TASM ..... Trusted Agent Security Manager

USAPA ..... United States Army Publishing Agency

USAG-AK ..... United States Army Garrison, Alaska and Fort Richardson (PROV)

USARAK ..... United States Army Alaska